Claude Chevalley

Modules

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. nº 2, p. 1-11
<http://www.numdam.org/item?id=SMJ_1933-1934__1__A2_0>

SEMINAIRE DE MATHEMATIQUES

Première année 1933-1934

Théorie des Groupes et des Algèbres

B.- Modules

Exposé fait par M. Claude CHEVALLEY, le lundi 25 Novembre 1933

<u>Définition du module</u> .- On appelle module un groupe abélien écrit sous forme additive . L'élément unité du groupe se représente par 0, et l'élément inverse d'un élément a par -a.

<u>Anneau</u> . - On appelle anneau un système σ d'éléments α, β...

jouissant des propriétés suivantes :

a) c'est un module

b) Il existe dans σ une seconde loi de composition, appelée multiplication, satisfaisant aux conditions suivantes :

A) associativité : $(\alpha\beta).\gamma = \alpha(\beta\gamma)$

B) distributivité : $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma \quad (\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$

1.- <u>MODULES PAR RAPPORT A UN ANNEAU</u>

Supposons qu'un module $\mathfrak{M}$ admette les éléments d'un anneau σ comme opérateurs, c'est-à-dire que, α étant dans σ et a dans $\mathfrak{M}$ αa soit un élément défini de $\mathfrak{M}$, et que, de plus, $\alpha(a+b) = \alpha a + \alpha b$

Supposons de plus que $(\alpha+\beta)a = \alpha a + \beta a \qquad (\alpha \subset \sigma,\ \beta \subset \sigma)$

Dans ces conditions, on dit <u>que $\mathfrak{M}$ est module par rapport à σ ou σ-module</u> (gauche si dans la multiplication d'un élément de σ par un élément de $\mathfrak{M}$ on écrit l'élément de σ à gauche).

Exemple : Si σ est l'anneau des entiers rationnels , tout module $\mathfrak{M}$ est σ-module. En effet, a étant dans $\mathfrak{M}$, et ν étant un entier, on pose

$$\text{Si } \nu > 0 \quad \nu a = \underbrace{a + a + \ldots + a}_{\nu \text{ fois}}$$

$$\text{Si } \nu = 0 \quad 0.a = 0 \qquad \text{Si } \nu < 0 \quad \nu a = -(-\nu)\, a$$

Convention.- Nous aurons dans cet exposé à considérer des modules par rapport à un certain anneau σ. Les seuls sous-modules que nous considérerons seront des sous-modules "permis" (c'est à dire qui sont aussi des σ-modules), de sorte que nous nous abstiendrons de le répéter à chaque fois. D'autre part les éléments des modules que nous considérerons seront désignés par des minuscules latines, ceux de σ par des minuscules grecques.

2.- ADDITION DES SOUS-MODULES

Considérons un module $\mathfrak{M}$ et des sous-modules $\mathfrak{N}_1, \mathfrak{N}_2 \ldots \mathfrak{N}_k$ de $\mathfrak{M}$. On appelle somme de ces sous-modules et on désigne par $\mathfrak{N}_1 + \mathfrak{N}_2 + \ldots + \mathfrak{N}_k$ le module composé des éléments de la forme $n_1 + n_2 + \ldots + n_k$ avec $n_i \subset \mathfrak{N}_i$ ($i = 1, 2, \ldots k$) Si d'ailleurs un élément de la somme ne se met que d'une manière sous la forme $n_1 + n_2 + \ldots + n_k$, $n_i \subset \mathfrak{N}_i$ la somme est dite directe et peut se représenter par $\mathfrak{N}_1 \oplus \mathfrak{N}_2 \oplus \ldots \mathfrak{N}_k \oplus$ Il faut et il suffit pour qu'il en soit ainsi que la condition $n_1 + n_2 + \ldots + n_k = 0$, $n_i \subset \mathfrak{N}_i$ entraine $n_1 = n_1 = \ldots = n_k = 0$

3.- IDEAUX

En vertu de l'existence de la multiplication, σ est lui-même $\mathfrak{o}$ -module gauche . Les $\mathfrak{o}$-modules gauches contenus dans $\mathfrak{o}$ sont appelés idéaux à gauche de $\mathfrak{o}$. On définit de même les idéaux à droite . Si la multiplication est commutative dans $\mathfrak{o}$, ces deux notions coincident .

Soit $\mathfrak{a}$ un idéal à gauche de $\mathfrak{o}$ et soit $\mathfrak{M}$ un $\mathfrak{o}$-module gauche . Si u est dans $\mathfrak{M}$, l'ensemble des produits des éléments de $\mathfrak{a}$ par u constitue un sous-module de $\mathfrak{M}$ qu'on désigne par $\mathfrak{a}$ u. De même si $\mathfrak{N}$ est un sous-module, l'ensemble des éléments de la forme $\alpha_1 n_1 + \alpha_2 n_2 + \ldots\ldots + \alpha_k n_k$ avec $\alpha_i \subset \mathfrak{a}$, $n_i \subset \mathfrak{N}$, constitue un sous-module qu'on désigne par $\mathfrak{a}\mathfrak{N}$. On a :

$$\mathfrak{a}(\mathfrak{N} + \mathfrak{N}') = \mathfrak{a}\mathfrak{N} + \mathfrak{a}\mathfrak{N}'$$

4.- BASE D'UN MODULE

A partir de maintenant, nous supposerons pour simplifier que $\mathfrak{o}$ contienne une unité 1, c'est à dire un élément tel que pour tout élément α de $\mathfrak{o}$ on ait $1.\alpha = \alpha.1 = \alpha$.
Nous supposerons de plus que les $\mathfrak{o}$- modules que nous considérerons seronts tels que 1.a =a pour tout a du module .

Si on peut trouver dans un $\mathfrak{o}$-module $\mathfrak{M}$ un système d'éléments x_1, x_2 ....., x_n tel que $\mathfrak{M} = \mathfrak{o}x_1 + \mathfrak{o}x_2 + \ldots + \mathfrak{o}x_n$ ces éléments seront dits constituer une base de $\mathfrak{M}$.
Si, de plus, la somme du second membre est directe, la base est dite minima . Pour cela, il faut et suffit que les x_i soient linéairement indépendants (par rapport à $\mathfrak{o}$) c'est-à-dire qu'il n'existe aucune égalité de la forme :

$\sum_1^n \alpha_i x_i = 0$ à coefficients α_i non tous nuls dans σ .

5.- CRITERE D'EXISTENCE D'UNE BASE

Supposons qu'un module $\mathfrak{M}$ ne possède pas de base . Définissons par récurrence $\mathfrak{M}_n$ de la manière suivante :

1) $\mathfrak{M}_1 = \sigma x_1$ où x_1 est un élément différent de 0 de $\mathfrak{M}$

2) $\mathfrak{M}_n$ étant défini et ayant une base (x_1 , x_2,.......x_n) n'est pas identique à $\mathfrak{M}$, on prend un élément x_{n+1} de $\mathfrak{M}$ non situé dans $\mathfrak{M}_n$ et on pose $\mathfrak{M}_{n+1} = \mathfrak{M}_n + \sigma x_n$, ce qui définit $\mathfrak{M}_{n+1}$ et démontre qu'il a une base . $\mathfrak{M}_{n+1}$ contient $\mathfrak{M}_n$ sans lui être identique

Donc $\mathfrak{M}$ ne satisfait pas au "TEILERKETTENSATZ" : Toute suite croissante de sous-modules ne contient qu'un nombre fini de termes .

On a donc démontré que :

Si un module $\mathfrak{M}$ satisfait au Teilerkettensatz, il possède une base.

La réciproque n'est pas vraie en général, mais elle est vraie dans le cas où σ considéré comme σ-module gauche, satisfait au Teilerkettensatz. On démontre en effet le théorème suivant (Van der Waerden, Moderne Algebra, t. II . p. 87)

Si satisfait au Teilerkettensatz, et si un σ -module y satisfait également, tout sous-module de $\mathfrak{M}$ possède une base

Les modules qui possèdent une base, sont souvent appelés finis .

CORPS

Un anneau $\mathfrak{K}$ s'appelle un corps quand il jouit de la propriété suivante : α, β étant des éléments de $\mathfrak{K}$, avec $\beta \neq 0$ il existe un élément γ et un seul tel que $\alpha = \gamma\beta$ et quand de plus il ne se réduit pas à l'élément 0

Les corps $\mathfrak{K}$ sont caractérisés par cette propriété qu'ils ne possèdent que deux idéaux à gauche distincts, à savoir (0) et $\mathfrak{K}$. Ils satisfont donc au Teilerkettensatz.

MODULES PAR RAPPORT A UN CORPS

Soit $\mathfrak{K}$ un corps, et soit $\mathfrak{M}$ un $\mathfrak{K}$-module fini. Répétons la construction faite au début du prg.5. La suite (x_1, x_2 ... s'arrête au bout d'un nombre fini n de termes. Les éléments x_1, x_2, ... x_n forment une base de $\mathfrak{M}$. Cette base est minima Supposons en effet qu'il existe une relation $\sum_1^n \alpha_i x_i = 0$ les α_i n'étant pas tous nuls. Soit α_{n_0} le dernier coefficient différent de 0. On a $x_{n_0} = -\alpha_{n_0}^{-1}\alpha_1 x_1 - \alpha_{n_0}^{-1}\alpha_2 x_2 - \cdots - \alpha_{n_0}^{-1}\alpha_{n_0-1} x_{n_0-1}$ ce qui est impossible.

Donc : Si $\mathfrak{K}$ est un corps, un $\mathfrak{K}$-module fini possède une base minima.

On démontre que le nombre des éléments d'une base est indépendant de cette base et égal au rang du module, c'est-à-dire au nombre maximum d'éléments linéairement indépendants du module.

8.- MODULES PAR RAPPORT A L'ANNEAU DES ENTIERS RATIONNELS

A partir de maintenant, $\mathfrak{o}$ désignera l'anneau des entiers rationnels , k le corps des nombres rationnels , et $\mathfrak{M}, \mathfrak{N}, \mathfrak{P}$.. des $\mathfrak{o}$ -modules finis .

On dit que $\mathfrak{M}$ est régulier si la condition

$$\nu a = 0 \quad \nu \subset \mathfrak{o} \qquad a \subset \mathfrak{M}$$

entraine que l'un des éléments ν, a est nul.

A) Etude des modules réguliers finis

Nous allons d'abord supposer $\mathfrak{M}$ régulier . On démontre d'abord bien facilement que $\mathfrak{M}$ est isomorphe à un module contenu dans un k-module fini $\mathfrak{M}_K$. Nous supposerons donc que $\mathfrak{M} \subset \mathfrak{M}_K$

Si $\mathfrak{M} \neq (0)$ soit u_1 un élément $\neq 0$ de $\mathfrak{M}$. On appelle coefficient de u_1 (par rapport à $\mathfrak{M}$) l'ensemble des éléments ξ de K tels que ξu_1 soit dans $\mathfrak{M}$. C'est un $\mathfrak{o}$-module qui est isomorphe à l'ensemble des ξu_1 donc qui est fini . Or :

Un $\mathfrak{o}$-module fini $\mathfrak{a}$ contenu dans k se compose des multiples d'un nombre rationnel ρ . On écrit $\mathfrak{a} = \mathfrak{o}\rho = (\rho)$

En effet, $\mathfrak{a}$ possède une base $(\xi_1 . \xi_2 .... \xi_K)$.
Il en résulte que les dénominateurs des nombres de $\mathfrak{a}$ (mis sous forme réduite) divisent le produit des dénominateurs des ξ_i . Il existe donc , dans $\mathfrak{a}$, (si $\mathfrak{a} \neq 0$) un nombre rationnel positif minimum ρ ; Soit ξ un élément quelconque de $\mathfrak{a}$; on a $\xi = \nu\rho + \rho'$, $\nu \subset \mathfrak{o}$ $\quad 0 \leq \rho' < \rho$
$\rho' = \xi - \nu\rho$ est dans $\mathfrak{a}$, d'où $\rho' = 0$ ce qui démontre la proposition .

Ceci posé, revenons au module $\mathfrak{M}$. Soit $\mathfrak{M}_1 = \sigma \rho u_1$.
$\mathfrak{M}/\mathfrak{M}_1$ est un module régulier. En effet, soit $v^* \subset \mathfrak{M}/\mathfrak{M}_1$ et soit v un élément de $\mathfrak{M}$ contenu dans la classe v^* (mod. $\mathfrak{M}_1$) Supposons $\lambda v^* = 0$; on a $\lambda v = \nu \rho u_1$, ν entier.
Si $\lambda \neq 0$, on a $v = \lambda^{-1} \nu \rho u_1$ et $v^* = 0$
Ceci conduit à la définition suivante :

<u>Un sous-module $\mathfrak{N}$ tel que $\mathfrak{M}/\mathfrak{N}$ soit régulier est dit primitif.</u> $\mathfrak{N}$ étant un sous-module primitif, nous allons montrer qu'il existe un autre sous-module $\mathfrak{R}$ tel que

$$\mathfrak{M} = \mathfrak{N} \oplus \mathfrak{R}$$

Définissons par récurrence des éléments v_0, v_1, v_2 ... de la manière suivante :

a) On a $v_0 = 0$

b) Si v_1, v_2, ..., v_i sont déjà définis, et si $\mathfrak{N}_i = \mathfrak{N} + \sigma v_1 + \sigma v_2 + \dots + \sigma v_i$ est primitif, soit u^*_{i+1} un élément $\neq 0$ de $\mathfrak{M}/\mathfrak{N}_i$ (s'il y en a ; sinon, v_{i+1} ne sera pas défini), et soit $\sigma \rho_{i+1}$ son coefficient par rapport à $\mathfrak{M}/\mathfrak{N}_i$
Soit u_{i+1} un élément de $\mathfrak{M}$ appartenant à la classe u^*_{i+1} (mod. $\mathfrak{N}_i$) . On pose $v_{i+1} = \rho_{i+1} u_{i+1}$, $\mathfrak{N}_{i+1} = \mathfrak{N}_i + \sigma v_{i+1}$
En vertu de l'un des théorèmes d'isomorphisme, on a

$$\mathfrak{M}/\mathfrak{N}_{i+1} \simeq (\mathfrak{M}/\mathfrak{N}_i)/\sigma \rho_{i+1} u^*_{i+1}$$

et par suite $\mathfrak{N}_{i+1}$ est primitif. La suite des modules $\mathfrak{N}_i$ est croissante et par suite, au bout d'un nombre fini n d'opérations, on sera arrêté, ce qui signifie que $\mathfrak{N}_n = \mathfrak{M}$
Posons $\mathfrak{R} = \sigma v_1 + \sigma v_2 + \dots + \sigma v_n$. Supposons qu'il exis-

te une relation de la forme $u + \sum_1^n \alpha_i v_i = 0$, avec $u \in \mathcal{R}, \alpha_i \in \sigma$
Soit α_{n_0} le dernier coefficient $\neq 0$ (s'il y en a). Dans $\mathcal{M} / \mathcal{N}_{n_0 - 1}$ on a $\alpha_{n_0} v^*_{n_0} = 0$, ce qui est impossible . Donc les α_i sont tous nuls et par suite aussi u. Donc on a :

$$\mathcal{M} = \mathcal{N} \oplus \mathcal{R} \qquad \text{et } v_1 , v_2 \ldots\ldots v_n$$

forment une base minima de $\mathcal{R}$.

Donc : Si $\mathcal{M}$ est σ-module régulier fini, et si $\mathcal{N}$ est un sous-module primitif, il existe un autre sous-module $\mathcal{R}$ tel que $\mathcal{M} = \mathcal{N} \oplus \mathcal{R}$. De plus, $\mathcal{M}$ possède une base minima

On démontre de plus facilement que le nombre des éléments d'une base minima de $\mathcal{M}$ est égal au rang de $\mathcal{M}$.

B) Etude des modules finis quelconques

Soit à partir de maintenant, $\mathcal{M}$ un σ-module fini quelconque . Soit $u_1 , u_2 , \ldots\ldots u_n$ une base de $\mathcal{M}$. Soit $\mathcal{N}$ le module des formes linéaires par rapport à n variables x_1, x_2, ... x_n à coefficients dans σ . La correspondance $\sum_1^n \alpha_i x_i \longrightarrow \sum_1^n \alpha_i u_i$ est une homomorphie . Donc $\mathcal{M}$ est homomorphe à $\mathcal{N}$ et par suite isomorphe au quotient $\mathcal{N} / \mathcal{R}$ de $\mathcal{N}$ par un de ses sous-modules $\mathcal{R}$. Or nous allons démontrer que :

Si $\mathcal{N}$ est un σ-module régulier fini, si $\mathcal{R}$ est sous-module de $\mathcal{N}$, il existe des bases minima (u_1 , u_2 , ...u_n) de $\mathcal{N}$ et (v_1 , v_2 , ...v_n) de $\mathcal{R}$ telles que $v_i = \varepsilon_i u_i$ (i = 1, 2,......r) les ε_i étant des entiers tels que ε_i divise ε_{i+1} .

Soit w un élément $\neq 0$ de $\mathcal{P}$ et soient $\sigma\rho, \sigma\sigma$ ses coefficients par rapport à $\mathcal{M}, \mathcal{P}$. On a $\sigma\sigma \subset \sigma\rho$ et par suite $\sigma = \nu_w \rho$, ν_w ~~ν_w~~ étant un entier (défini par w au signe près ; nous le supposerons > 0) qu'on appelle <u>coefficient relatif</u> de w. Désignons par $\overline{u}$ l'homologue dans $\mathcal{M}/\mathcal{P}$ d'un élément u de $\mathcal{M}$. Alors ν_w est le plus petit entier ν positif tel que $\nu\,\overline{\rho.w} = 0$. On voit tout de suite que les éléments $\overline{u}$ de $\mathcal{M}/\mathcal{P}$ tels que $\nu\,\overline{u} = 0$ (ν étant un entier fixe) forment un sous-module de $\mathcal{M}/\mathcal{P}$ qui ne peut qu'augmenter quand on remplace ν par un multiple. Il en résulte, en vertu du Teilerkettensatz dans $\mathcal{M}/\mathcal{P}$ que les coefficients relatifs des éléments w de $\mathcal{P}$ divisent tous un entier fixe δ. Soit $\delta = \prod_1^h \varpi_i^{u_i}$ la décomposition de δ en facteurs premiers. Soit d'autre part ε, le p.g.c.d. de tous les coefficients relatifs ν_w. On a $\mathcal{P} \subset \varepsilon\mathcal{M}$, mais $\mathcal{P} \not\subset \xi\varepsilon\mathcal{M}$ si ξ est un entier > 1. Déterminons un élément w_i de $\mathcal{P}$ tel que :

$$w_i \notin \varpi_i \varepsilon \mathcal{M} \quad (i = 1, 2, \ldots h)$$

et soit φ_i un entier tel que :

$$\varphi_i \equiv 1 \ (\mathrm{mod.}\ \varpi_i) \qquad \varphi_i \equiv 0 \ \left(\mathrm{mod.}\ \frac{\delta}{\varpi_i^{u_i}}\right)$$

Soit $w = \sum_1^h \varphi_i w_i$. w n'est contenu dans aucun des modules $\varpi_i \varepsilon \mathcal{M}$ et par suite $\frac{\nu_w}{\varepsilon}$ n'est divisible par aucun des ϖ_i. Comme ce nombre divise δ, il est égal à ± 1 et même à $+1$ car ν_w et ε sont positifs.

Ceci posé, le théorème à démontrer est à peu près évident si n= 1 . Supposons-le démontré pour les modules $\mathfrak{M}$ ayant une base minima composée de moins de n éléments . w étant un élément déterminé comme nous venons de le dire, soient $\sigma\rho$, $\sigma\sigma$ ses coefficients par rapport à $\mathfrak{M}, \mathfrak{P}$

Posons $\rho w = u_1$ $\sigma w = v_1$. σu_1 est , comme on l'a démontré dans A) un sous-module primitif de $\mathfrak{M}$; il existe donc un module $\mathfrak{M}_1$ tel que $\mathfrak{M} = \sigma u_1 \oplus \mathfrak{M}_1$

Soit u un élément de $\mathfrak{P}$; comme $u \subset \varepsilon \mathfrak{M}$ on a $u = \varepsilon \alpha u_1 + v$ ou $\alpha \subset \sigma$, $v \subset \mathfrak{M}_1$ Mais $\varepsilon u_1 = v_1 \subset \mathfrak{P}$. donc $v \subset \mathfrak{P}$

Les éléments de $\mathfrak{P}$ contenus dans $\mathfrak{M}_1$ forment un sous-module $\mathfrak{P}_1$ et on a , d'après ce qu'on vient de voir, $\mathfrak{P} = \sigma v_1 \oplus \mathfrak{P}_1$

D'autre part, $\mathfrak{M}_1$ possède une base composée de n-1 éléments. Donc on peut trouver une base minima (u_2, ...u_n) de $\mathfrak{M}_1$ et une base minima (v_2, ...v_n) de $\mathfrak{P}_1$ telles que

$v_i = \varepsilon_i u_i$, ε_i divisant ε_{i+1} (i = 2, ...r)

D'ailleurs, $\mathfrak{P} \subset \varepsilon \mathfrak{M}_1$ ce qui montre que les ε_i sont divisibles par ε_1 . Le théorème est donc démontré .

On en déduit la structure de $\mathfrak{M} / \mathfrak{P}$ et par suite le théorème suivant :

<u>Si $\mathfrak{M}$ est un σ-module fini, on peut y trouver n éléments u_1, u_2, ... u_n tels que tout élément de $\mathfrak{M}$ se mette , et d'une seule manière, sous la forme $\sum \alpha_i u_i$, avec les conditions $0 \leq \alpha_i < \varepsilon_i$ (i = 1, 2, ...r).</u>

On peut encore dire que :

$\mathfrak{M}$ est somme directe d'un certain nombre de modules de la forme σu .

Ces derniers sont souvent appelés , par analogie avec la théorie des groupes, modules cycliques.

Enfin, on a obtenu le théorème suivant de la théorie des groupes :

Un groupe abélien possédant un système d'un nombre fini de générateurs (en particulier un groupe abélien fini) est produit direct de groupes cycliques.

On remarquera que les méthodes de démonstration employées s'appuient exclusivement (à des détails près) sur les faits suivants : σ ne possède pas de diviseur de zéro , est commutatif et tous les idéaux de σ sont principaux, c'est-à-dire de la forme $\sigma\rho$. Les théorèmes sont donc vrais pour tous les anneaux satisfaisant à ces conditions . Ils se généralisent d'ailleurs encore pour des classes beaucoup plus vastes d'anneaux .
